บทที่ 9
บทวิจารณ์และสรุปผล

โครงงานชิ้นนี้ เป็นการพัฒนาต้นแบบประยุกต์ชิปเข้าและถอดรหัส ซึ่งเป็นการนำอุปกรณ์ฮาร์ดแวร์มาทำการเข้าและถอดรหัส โดยสามารถทำงานข้ามเครือข่ายได้ด้วยระบบวีพีเอ็น (VPN) และทำการเขียนดีไวซ์ไดรเวอร์ขึ้น เพื่อช่วยให้ตัวฮาร์ดแวร์ทำงานได้อย่างมีประสิทธิภาพมากขึ้น

9.1 การวิจารณ์โครงงาน

เนื่องจากโครงงานนี้ เป็นต้นแบบในการใช้งานชิปเข้าและถอดรหัสข้อมูล จึงเป็นการทำงานที่ใหม่หมด ซึ่งต้องทำการศึกษาทั้งหมด

9.1.1 ส่วนที่เกี่ยวข้องกับฮาร์ดแวร์

ในส่วนของการพัฒนาในด้านฮาร์ดแวร์นั้น ต้องใช้ความรู้และความเข้าใจอยู่หลายส่วน ทั้งเรื่องของตัวบอร์ดเอฟพีจีเอ การ์ดไอเอสเอ และส่วนของโปรแกรมที่ใช้โหลดลงบอร์ด ซึ่งการพัฒนาในด้านฮาร์ดแวร์นั้น มีความสลับซับซ้อนและยุ่งยาก

- บอร์ดเอฟพีจีเอที่ทำหน้าที่เข้ารหัส

ในด้านของการเขียนโปรแกรมภาษาวีเอชดีแอล (VHDL) ที่ทำหน้าที่ในการเข้าและถอดรหัสข้อมูล ได้เกิดปัญหาที่เหนือการแก้ไขได้อยู่ คือ ภาษาวีแอชดีแอลที่ยังมีข้อจำกัดบางอย่างซ่อนอยู่ เช่น ข้อจำกัดในเรื่องของไอโอ (I/O) เรื่องคล็อก (Clock) เรื่องขนาดของ H-Function ที่มีจำนวนน้อย และเรื่องอื่น ๆ และอัลกอริทึม DES ที่กำหนดไว้ตอนแรกนั้น ตัวโปรแกรมมีขนาดใหญ่เกินที่จะโหลดลงบอร์ดเอฟพีจีเอได้ จึงต้องทำการเปลี่ยนอัลกอริทึมการเข้าและถอดรหัส

- การ์ดไอเอสเอ

ในส่วนของการ์ดไอเอสเอที่ทำหน้าที่เชื่อมการทำงานระหว่างเครื่องคอมพิวเตอร์กับตัวบอร์ดเอฟพีจีเอ ยังคงมีปัญหาในเรื่องการทำงานของไอซีบางตัว ที่ทำงานได้ไม่ทันกับการทำงานของบอร์ดเอฟพีจีเอ และปัญหาในด้านการดีบัก (Debug)

9.1.2 ส่วนที่เกี่ยวข้องกับซอฟต์แวร์

ในส่วนของการพัฒนาซอฟต์แวร์ คือ ส่วนที่ทำการเพิ่มเข้ามาเพื่อทำให้การทำงานของอุปกรณ์ต้นแบบทำงานได้อย่างมีประสิทธิภาพและสะดวกสบายมากขึ้น

- ดีไวซ์ไดรเวอร์

ปัญหาที่เกิดขึ้นในการเขียนดีไวซ์ไดรเวอร์ คือ ความเข้าใจในด้านการทำงานของไดรเวอร์และการออกแบบโปรแกรมของไดรเวอร์ เนื่องจากการเขียนดีไวซ์ไดรเวอร์นั้น สลับซับซ้อนและยากที่จะเข้าใจได้ง่าย

- วีพีเอ็น

เป็นปัญหาในด้านการรับและส่งข้อมูล

9.2 สรุปผลของโครงงาน

โครงงานนี้ เป็นต้นแบบประยุกต์การใช้งานชิปเข้าและถอดรหัส และจากที่ได้ทำการออกแบบและการทดลองแล้ว ผลที่ได้ออกมา คือ ต้นแบบสามารถทำงานได้จริง ทั้งการเข้าและถอดรหัสข้อมูลและการรับ-ส่งข้อมูลระหว่างเครือข่ายที่เมื่อมีการดักจับข้อมูลระหว่างที่ส่งแล้ว ผู้ดักจับไม่สามารถทำการตีความหมายข้อมูลนั้น ๆ ได้

9.3 แนวทางการพัฒนาต่อไปในอนาคต

- เปลี่ยนแปลงในด้านของอัลกอริทึมที่นำมาใช้ในการเข้าและถอดรหัสจาก XOR ธรรมดาให้เป็นอัลกอริทึมอื่นที่มีความสลับซับซ้อนมาขึ้นกว่า เพื่อเพิ่มประสิทธิภาพความปลอดภัยให้แก่ข้อมูล